

[NT] Windows 2000 ShellExecute() API Lets Applications to Cause a Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0013.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/03/03

To: list@securiteam.com

Date: 3 Jul 2003 12:09:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Windows 2000 ShellExecute() API Lets Applications to Cause a Buffer Overflow

SUMMARY

A buffer overflow vulnerability exists in the Windows 2000 API function ShellExecute(). The vulnerability would allow attackers to use web browsers, MUAs, text editors, etc to cause the overflow to occur.

DETAILS

Vulnerable systems:

* SHELL32.DLL (Version 5.0.3502.6144)

Windows API ShellExecute() is a function to run an application associated with a specified file extension.

The problem is triggered when the pointer to an unusually long string is set to the 3rd argument of the Windows 2000 API ShellExecute() API function.

Securiteam: [NT] Windows 2000 ShellExecute() API Lets Applications to Cause a Buffer Overflow

It has been confirmed that several applications containing web browser, MUA and text editor are vulnerable to this problem.

Solution:

This problem can be rectified by installing Windows 2000 Service Pack 4 that can be downloaded from:

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>
<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>

ADDITIONAL INFORMATION

The information has been provided by <mailto:y.arai@lac.co.jp> Yuu Arai and Hisayuki Shinmachi (<mailto:snsadv@lac.co.jp> Secure Net Service(SNS) Security Advisory).

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.